CLAIMS

What is claimed is:

1. A method for automatically creating a record for one or more security incidents and reactions thereto, comprising the steps of:

recording security incident information with at least one of a date and time stamp;

providing data to enable display of a procedure;

receiving a selection of a procedure;

executing the selected procedure;

in response to executing the selected procedure, recording executed procedure information and results of the executed procedure with at least one of a date and time stamp; and

outputting a record comprising the security incident information, executed procedure information, results of one or more executed procedures, an identity of a user who selected the procedure, and at least one of a corresponding date stamp and time stamp.

2. The method of claim 1, wherein the record comprises an unmodifiable, permanent database.

3. The method of claim 1, further comprising the step of recording the results of the executed procedure with a digital signature to enable detection of any modification of the recorded results, whereby integrity of the recorded results can be monitored.

4. The method of claim 1, further comprising the step of extracting information from the results of an executed procedure.

5. The method of claim 4, further comprising the step of describing a security incident with said extraction information.

6. The method of claim 1, further comprising the step of displaying information for a particular security incident to more than one user.

7. The method of claim 1, further comprising the step of prepopulating fields of a record of a first program module from a second program module.

8. The method of claim 1, further comprising the steps of:

receiving security incident information from a first program module;

processing the security incident information with a second program module; and

forwarding the processed security incident information from the second program module to a third program module.

9. The method of claim 1, wherein the step of receiving a selection of a procedure comprises automatically selecting a procedure with a program module.

10. The method of claim 1, further comprises the step of suggesting a procedure with a program module based upon the type of security incident.

11. The method of claim 1, wherein each step is performed automatically by a program module.

12. The method of claim 1, wherein some of the steps are performed automatically by a program module.

13. The method of claim 1, further comprising the step of displaying reports comprising one or more computer security incidents.

14. The method of claim 1, wherein the results of an executed procedure comprise at least one of text, numbers, images, or formatted documents.

15. The method of claim 1, further comprising the step of predicting future actions of a source of a security incident.

16. The method of claim 1, further comprising the step of identifying the source of a security incident.

17. The method of claim 1, further comprising the step of sorting decoy or false security incidents from actual security incidents.

18. The method of claim 1, further comprising the step of linking a first procedure to a second procedure.

19. The method of claim 1, further comprising the step of determining the authorization level of a user.

20. The method of claim 1, wherein the step of providing data to enable display of a procedure further comprises the step of providing data for enabling display of one or more steps of a procedure.

21. The method of claim 1, further comprising the steps of:

providing data to enable display of a response procedure;

executing the response procedure; and

in response to executing the response procedure, recording executed response procedure information and results of the executed response procedure with at least one of a date and time stamp.

22. The method of claim 1, further comprising the steps of:

providing data to enable display of an investigation procedure;

executing the investigation procedure; and

in response to executing the investigation procedure, recording executed investigation procedure information and results of the executed investigation procedure with at least one of a date and time stamp.

23. The method of claim 21, wherein the step of providing data to enable display of the response procedure further comprises the step of providing data to enable display of one or more steps of the response procedure.

24. The method of claim 1, further comprising the step of providing data to enable display of results of the executed procedure.

25. The method of claim 23, further comprising the step of providing data to enable display of results of the executed response procedure.

26. The method of claim 1, further comprising the steps of:

identifying an appropriate computer to execute a step in the investigation procedure; and

identifying an appropriate computer to execute a step in the response procedure.

27. The method of claim 26, further comprising the steps of:

accessing a table comprising computer locations and step information;

comparing a step to be executed with computer locations listed in the table;

determining if a match exists between the step to be executed and the computer locations; and

if one or more matches exist, displaying the matching information or automatically selecting an appropriate location.

28. The method of claim 27, wherein the table further comprises Internet address ranges, the method further comprising the step of comparing an Internet address of a source of a security incident with the Internet address ranges of the table.

29. The method of claim 27, further comprising the step of providing data to enable display of an appropriate substitute computer location if a match does not exist.

30. The method of claim 27, further comprising the step of identifying an appropriate computer to execute a step in either an investigation or a response procedure, wherein the computer is strategically located relative to a source of a security incident.

31. The method of claim 1, wherein each procedure comprises one or more steps, the method further comprising the step of executing one or more program modules in response to a selection of a procedure.

32. The method of claim 31, wherein the one or more program modules comprise one or more software application programs that can operate as stand alone programs.

33. The method of claim 31, wherein at least one program module comprises an off-the-shelf software application program.

34. The method of claim 1, wherein the security incident information comprises predefined attributes.

35. The method of claim 34, wherein the predefined attributes comprise any one of a computer incident severity level, a computer incident category, a computer incident scope value, a computer incident status value, an attacker internet protocol (IP) address value, an attacker ISP name, an attacker country, an external attacker status value, an incident type value, a vulnerabilities level, an entry point value, an attack profile value, a target networks value, a target firewalls value, a target hosts value, a target services value, a target accounts value, and a damage type value.

36. The method of claim 1, wherein the security incident information comprises attributes that are at least one of variable and computer-generated.

37. The method of claim 35, further comprising the step of determining whether a security incident comprises an actual breach in security based upon values of its attributes.

38. The method of claim 1, further comprising the steps of:

receiving a selection for a step of a procedure; and

generating a pre-execution warning prior to the selection of a step.

39. The method of claim 1, further comprising the steps of:

receiving a selection for a step of a procedure;

executing the selected step; and

suggesting an appropriate subsequent step in the procedure.

40. The method of claim 1, wherein each step is performed automatically in response to a detected computer security incident.

41. The method of claim 1, further comprising the steps of:

providing data to enable display of a plurality of computer tools in a non-procedural manner;

receiving a selection for a computer tool; and

executing the selected computer tool.

42. A method for organizing and recording reactions to one or more computer security incidents, comprising the steps of:

providing data to enable display of one or more security investigation procedures;

providing data to enable display of one or more security response procedures;

in response to a selection of a security investigation procedure, providing data to enable display of one or more corresponding investigation steps;

in response to a selection of a security response procedure, providing data to enable display of one or more corresponding response steps; and

generating a permanent record comprising security incident information, executed investigation step and result information, executed response step and result information, and corresponding date and time stamps.

43. The method of claim 42, further comprising the step of recording executed investigation step information and results of the executed investigation step with at least one of a date and time stamp in response to a selection of a step of an investigation procedure.

44. The method of claim 42, further comprising the step of recording executed response step information and results of the executed response step with at least one of a date and time stamp in response to a selection of a step of a response procedure.

45. The method of claim 42, further comprising the steps of:

providing data to enable display of a plurality of procedures;

in response to receiving a selection of a procedure, displaying a plurality of steps;

obtaining modification information for the selected procedure; and

storing the modification information.

46. The method of claim 42, further comprising the step of at least one of adding or deleting a step in a procedure.

47. The method of claim 42, further comprising the steps of:

providing data to enable display of a plurality of steps of a procedure;

in response to selection of a step, providing data to enable display of detailed information fields related to the selected step;

obtaining modification information for the selected step; and

storing the modification information.

48. The method of claim 42, further comprising the step of at least one of adding, deleting, or modifying a step in a procedure.

49. The method of claim 42, further comprising the steps of:

obtaining computer security incident search information; and

providing data to enable display of one or more computer security incidents matching the computer security incident search information.

50. The method of claim 42, further comprising the steps of:

tracking multiple computer security incidents; and

storing information for each computer security in accordance with at least one of date and time stamp.

51. A method for selecting a computer that is strategically located relative to a source of a security incident, comprising the steps of:

accessing a table comprising computer locations, Internet address ranges, and security step information;

comparing a security step to be executed and a target Internet address with computer locations and Internet address ranges listed in the table;

determining if a match exists between the security step to be executed and the computer locations;

determining if a match exists between an Internet address of a security incident and the Internet address ranges listed in the table; and

selecting a computer to execute the security step based upon the matching steps, wherein the computer has a location and is capable of interacting with the Internet address of the security incident.

52. The method of claim 51, further comprising the step of:

if one or more matches exist, providing data to enable display of the matching information;

if a match does not exist, providing data to enable display of one or more appropriate substitute computer locations or automatically selecting an appropriate location.

53. The method of claim 51, wherein the security step comprises a portion of a security response procedure, wherein the computer is strategically located relative to a source of a security incident.

54. The method of claim 51, wherein the step comprises a portion of a security investigation procedure, wherein the computer is strategically located relative to a source of a security incident.

55. The method of claim 51, wherein each step to be executed in a security procedure comprises one or more off-the-shelf security application programs.

56. A method for generating a permanent record of one or more computer security incidents and reactions thereto, comprising the steps of:

displaying one or more tools;

receiving a selection of a tool;

in response to a selection of a tool, forwarding data for execution of the tool; and

forwarding data for generating a permanent record comprising security incident information, executed tool information, and corresponding date and time stamps.

57. The method of claim 56, further comprising the step of displaying the tools as icons on a computer display.

58. The method of claim 56, further comprising the step of displaying a plurality of tools that are selectable from a menu.

59. The method of claim 31, further comprising the step of installing the one or more program modules within a single program on a server.

60. The method of claim 31, further comprising the step of installing the one or more program modules on a single server.

61. The method of claim 31, further comprising the step of installing the one or more program modules on a computer that is a target of a computer incident.

62. The method of claim 31, further comprising the step of installing the one or more program modules on both a computer that is a target of a computer incident and a server.

63. The method of claim 27, wherein the table further comprises Internet address ranges, the method further comprising the step of comparing an Internet address of a computer subject to an attack or security breach with the Internet address ranges of the table.

64. The method of claim 27, wherein the table further comprises Internet address ranges, the method further comprising the step of comparing an Internet address of a witness to a security incident with the Internet address ranges of the table.

65. The method of claim 27, wherein the table further comprises Internet address ranges, the method further comprising the step of comparing an Internet address of an accomplice to a security incident with the Internet address ranges of the table.